~~CONFIDENTIAL~~

FM 30-17A

FIELD MANUAL

COUNTERINTELLIGENCE SPECIAL OPERATIONS (U)

~~NATIONAL SECURITY INFORMATION~~
~~Unauthorized Disclosure~~
~~Subject to Criminal Sanctions~~

HEADQUARTERS, DEPARTMENT OF THE ARMY

FEBRUARY 1973

~~CONFIDENTIAL~~

~~Classified by Commander, CDC~~
~~Exempt from General Declassification~~
~~Schedule of Executive Order 11652~~
~~Exemption Category 3~~
~~Declassify on Indefinite~~

FIELD MANUAL
NO. 30-17A

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, D.C., *28 February 1978*

COUNTERINTELLIGENCE SPECIAL OPERATIONS (U)

*This manual supersedes FM 30-17A, 28 February 1968, including all changes.

CHAPTER 1

GENERAL

Section I. INTRODUCTION

1-2. (U) Changes

Users of this manual are encouraged to submit recommendations to improve its clarity or accuracy. Comments should be keyed to the specific page, paragraph and line of the text in which the change is recommended. Reasons should be provided for each comment to insure understanding and complete evaluation. Comments should be prepared using DA Form 2028 (Recommended Changes to Publications) and forwarded direct to the Commanding Officer, US Army Combat Developments Command Intelligence Agency, Fort Huachuca, Arizona 85613. Originators of proposed changes which would constitute a significant modification of approved Army doctrine may send an information copy, through command channels, to the Commanding General, US Army Combat Developments Command, Fort Belvoir, Virginia 22060, to facilitate review and followup.

Section II. HOSTILE INTELLIGENCE

1-4. (U) Introduction

The key to effective counterespionage, countersubversion, and countersabotage is to "know your enemy." Newly assigned counterintelligence personnel must first familiarize themselves thoroughly with hostile intelligence activities, methods of operation, agencies, and personalities common to the area in which they must operate. With unlimited resources, funds, and professionally skilled case officers or principal agents, counterintelligence special operations may become very sophisticated, using the latest technological developments. Conversely, the methods may be as simple as recruiting someone to observe the "enemy" and report on everything he sees or hears. Methods and techniques are also modified to meet the requirements posed by the effectiveness of opposing counterintelligence forces.

1-5. (U) Characteristics of Hostile Intelligence Activities

a. Predominant among the hostile intelligence services faced by US Forces are those of the USSR. The services of satellite nations are either patterned after the Soviet intelligence services or operate in a similar manner. A discussion of these methods is included as appendix B.

b. Insurgent movements will probably have an intelligence network patterned after the North Vietnamese apparatus particularly in newly developing countries. FM 30-31 should be referred to in insurgency situations.

1-6. (U) Functions of Counterintelligence

Counterintelligence is that phase of intelligence covering all activity devoted to destroying the effectiveness of inimical foreign intelligence activities. It also protects information against espionage, personnel against subversion, and installations and material against sabotage. Counterintelligence special operations are activities which have peacetime and wartime applications since they are used to gain knowledge about enemy intentions before, during, and after hostilities.

1-8. (U) Countersubversion

Countersubversion includes operations designed to detect, prevent, or neutralize the activities of subversive groups and individuals. The countersubversion mission may be limited to designated defensive and preventive measures within the confines of Army installations. In other cases it may be all encompassing, to include offensive measures directed toward the origin of hostile subversive plans and policies (chap 3).

1-9. (U) Countersabotage

Countersabotage operations are the most difficult of all counterintelligence special operations to manage. This is due to the highly compartmentation of sabotage cells or teams; the high security required for saboteurs; and the fact that such operations normally stem from incidents instead of personnel actions (chap 4).

Section III. TECHNICAL SUPPORT

1-10. (U) General

In both defensive and offensive counterintelligence measures described in this manual, technical methods or support may be employed within prescribed limitations (AR 381-17). Technical specialists should be included in operational briefings and planning so that they may give advice on available technical support and make specific recommendations for the special operations concerned. Special equipment can be acquired and must be accounted for as prescribed by AR 381-143.

Section IV. TERRORISM

3-11. (U) General

a. Terrorism is normally employed in an insurgency as a part of the subversive arm of the revolution. Terrorism is used as a tactical and/or strategic weapon whereby the populace is frightened into neutrality in the conflict, into cooperation with the insurgent, or into joining the insurgent force, overtly or covertly. Terrorism employed against an armed force can make it redeploy combat troops out of the field and into a security mission, exhaust its resources by attempting to hunt down the terrorists, overextend its lines of communication, and divert its energies into other directions.

b. Terrorism, in an insurgency, will tend to be less sophisticated than terrorism in a conventional conflict, therefore, those portions of chapter 4 which pertain to sabotage in rear areas during a conventional conflict, are also applicable to terrorist tactics.

c. Terrorism can be, and sometimes appears to be, a hit and miss, haphazard, seemingly patternless series of acts. In most instances, however, terrorism campaigns are as fully organized and planned as are sabotage campaigns. Therefore, every effort must be made to analyze incidents of a potential terrorism nature to detect the pattern if one exists. One area to scrutinize is the terrorists route into and out of the area. In addition, all people in the area should be interviewed in order to establish methods of operation, and descriptions of the terrorists. An indentikit can be most useful, particularly with illiterate individuals. This information, MO and individual descriptions, must be widely disseminated among sources and security forces in order to counteract the terrorism.

CHAPTER 4
COUNTERSABOTAGE

Section I. GENERAL

4-1. (U) Introduction

a. Sabotage is any act with an intent to damage, interfere with, or obstruct by willfully damaging or destroying or attempting to damage or destroy material, premises or utilities, in the interests of a foreign power or subversive political organization.

b. Countersabotage, then, is any action designed to destroy the effectiveness of foreign sabotage activities through the process of identifying, penetrating and manipulating, neutralizing or repressing individuals, groups or organizations conducting or capable of conducting such activities.

c. The crime of sabotage is discussed under Title 18, United States Code, chapter 105, sections 2151 2156 and is complex and not simply defined. This crime can occur in peacetime or wartime; however, it is more common during war. In a peacetime environment, any willful act or attempt of omission or commission committed with the specific intent to interfere with, damage, or destroy portions of the national defense effort and in the interest of a foreign power or subversive group is sabotage. In wartime, the peacetime definition applies and, additionally, a willful act of omission or commission committed by a person who is deemed to have "reason to believe" that his act may adversely affect the warmaking potential can be convicted of sabotage. During wartime, and particularly during internal defense or limited war situations, care must be taken to distinguish those acts involving clandestine enemy agents or dissatisfied friendly personnel from overt acts of war perpetrated by armed enemy units.

d. The use of sabotage against military targets can be expected to increase greatly prior to and during any future conflict in which US forces are involved. Developments in technology have increased the destructive power of sabotage devices while miniaturizing the size of their component parts.

e. The specific countersabotage responsibility assigned to a unit varies with the area, military situation, jurisdictional agreements, and directives. During and since World War II, sabotage has been directed mainly against material and facilities which support the military effort. Accordingly, the countersabotage role will be extensive in most cases and may require the employment of a significant portion of available counterintelligence resources in theaters of operations.

f. To successfully fulfill countersabotage responsibilities, counterintelligence personnel must have, in addition to complete understanding of installation and personnel security, a thorough knowledge of sabotage organizations, methods, capabilities, and limitations. They must be able to recognize an act of sabotage, understand its relationship to hostile objectives, analyze patterns of sabotage activity, and engage in defensive and offensive operations designed to prevent or neutralize sabotage activities.

4-2. (U) Sabotage Targets

The planning and implementation of a countersabotage program requires a thorough understanding of the procedures used by sabotage organizations in selecting sabotage targets. Major sabotage targets include natural resources, transportation, communications, power, fuel, industrial and military facilities, and equipment. All are susceptible to damage which could substantially impede their primary functions and are considered highly lucrative to a saboteur because their destruction or incapacitation may have a serious effect on morale, strategic capability, or combat effectiveness.

a. Target Selection Factors. In selecting a target, the sophisticated sabotage organization must consider several factors in relation to the capabilities of available saboteur personnel and the inherent risks required to perform the task; however, a terrorist cell may only be concerned with (2) and (3), below:

(1) *Value.* The strategic and tactical value must be considered. For example, the relative tactical value of disrupting the supply system or communications lines during a combat engagement may be weighed; or the strategic importance of destroying either research or production facilities may be considered. Related to the value of a target is its capability for recovery and the availability of other facilities to assume the mission or functions of the selected target.

(2) *Accessibility.* The availability of access depends chiefly upon the amount and type of security maintained and the geographic location.

(3) *Vulnerability.* Nearly all materiel and facilities are vulnerable to sabotage. The degree of vulnerability to destruction, however, varies and is an important factor in target selection. Some targets have an inherent capability to destroy themselves once a relatively small sabotage device is ignited.

(4) *Availability of sabotage materials.* The procurement, transportation, and storage of some types of explosives; and chemical, biological, or nuclear devices will present special problems for some types of sabotage activity. However, in most instances it can be anticipated that the sabotage organization will be able to provide the materials required for the particular means most suitable for a particular target.

b. Special Target Vulnerabilities. Those targets particularly vulnerable to sabotage, which are of sufficient importance to warrant sabotage consideration are discussed in FM 19-30. Additional targets are listed below:

(1) Land transportation systems: power systems; loading, transfer, and repair plants; and the road nets.

(*a*) Air transportation: aircraft, gasoline and lubricants, or runways.

(*b*) Water transportation: destruction of many vital components of the ship, piers, canal locks, blocking harbors, or navigational equipment and aids.

(*c*) Rail transportation: track system, tunnels, bridges, switches, or signal can be reversed.

(*d*) Bridges attacked by sabotage are normally limited to those with less than 12-inch girders. Split charges, on each side of the girder, one slightly above the other to give a scissor effect, are used. Railway bridges can be destroyed by the train detonating preset charges.

(*e*) Rolling stock: brake hoses, freight cars, gasoline tankers; and locomotive cylinders, fireboxes, brakeshoes, connecting rods, or air compressors.

(*f*) Railroad repair and transfer points: roundhouse turntables, locomotive brakes, hydraulic or electric switches in marshalling yards, warehouses, and cranes.

(2) Machinery is a vital element in all transportation, communications, and power systems, as well as in manufacturing. Nearly all types can be readily sabotaged. The simplest means is to interfere with lubrication by draining oil, damaging automatic lubricator and oil pipes, substituting improper viscosity oils, or by introducing abrasives into the system. Sensitive vital parts, particularly valves can be smashed or steel fragments can be dropped into moving parts or cylinders of engines. Explosives, too, are effective when placed in proximity to bearing pedestals, cast iron surfaces, or vital components and inside closed spaces.

(3) Fuel and power are essential to all transportation, communication, and manufacturing. Consequently, they are important sabotage targets.

(*a*) Hydroelectric systems are vulnerable to explosives at underwater parts of dams and sluice gates, turbines, governor gears, generators, pipelines, and valves.

(*b*) Steam powerplants can be attacked with explosives at coal-loading cranes and winches, the motor, gears, and supports of coal conveyers, cast iron links of stokers, bearing pedestals or iron casting surfaces of turbogenerators, feet and inspection doors of cast iron condensers, pumps, and water-cooling towers.

(*c*) Gas plant production may be stopped by damaging the retort stanchion supports for the distillation tubes, suction pumps, or the motor, gearbox, or supports for the coal conveyor.

(4) Factories can be incapacitated by burning records and stores, stealing or smashing jigs and patterns, cutting off power, or destroying loading and moving gear.

4-3. (U) Counterintelligence Responsibilities

Counterintelligence elements will have varying degrees of responsibilities for the detection, prevention, and neutralization of sabotage activity. The specific countersabotage responsibility assigned to a counterintelligence element will depend on the area, military situation, and jurisdictional or status-of-forces agreements. This role will be extensive in most cases and may require the employment of a significant portion of available resources in theaters of operation.

Section II. TYPES OF SABOTAGE

4-4. (U) Chemical, Biological, and Nuclear Sabotage

Chemical and biological agents, as well as prepositioned nuclear devices, may be used as means of committing sabotage in future wars or insurgency situations short of war.

a. Chemical Agents. Chemical agents can produce effects ranging from highly lethal to mildly incapacitating. Chemical compounds may be employed by a saboteur to produce a deep sleep for hours; psychochemical agents which produce confusion and inability to carry out orders; poisons which enter the

body by absorption and are lethal; and drinking water can very easily be contaminated with chemicals sufficiently potent to cause death. Initial delivery of chemical agents must be of a sufficient quantity to achieve the desired effect. Factors of dispersion and dilution will reduce the potency of the chemical agent. Therefore, to be effective, the agent must be delivered to the target in the necessary strength to accomplish what is desired before the agent dissipates. Aerosols, capsules, vials, special types of weapons, and spreading chemicals carried by the wind and dust are means of disseminating chemical agents.

b. Biological Operations. Biological operations are the employment of biological agents to produce casualties in man or animals and damages to plants or materials. Biological agents, when employed by a trained saboteur, have great sabotage potential.

(1) Biological agents are microorganisms which cause disease in man, plants, or animals, or cause the deterioration of material. Such microorganisms, grown, cultivated and introduced by man, are a deadly weapon which can enter humans through inhalation or through eating, and cannot be readily detected by the five senses. Further, it may be days rather than hours before disease symptoms caused by the microorganisms become apparent.

(2) There are many devices for spreading biological agents. Use and methods of such devices are limited only by the ingenuity of the saboteur and the desired effect. The saboteur's devices may consist of vials, capsules, various sizes of aerosol bombs, and specially designed devices with delaying mechanisms. Under favorable conditions microorganisms may be placed in old tin cans, bottles, and boxes around an area from which the microorganisms may multiply and spread. An aerosol bomb placed in an air intake ventilation system is a quick and easy method of spreading the agents throughout an entire building.

c. Nuclear Devices. Prepositioned nuclear devices may also be tools of the saboteur. Nuclear devices have great destructive capabilities and will destroy lives, crops, property, industrial sites, material, and equipment. A hostile nation may plan the use of small nuclear devices to create panic and undermine the morale of the citizens. Additional information is contained in AR 380-150 and in FM 19-30.

4-5. (U) Incendiary Sabotage

Fire is a very destructive type of sabotage and is easily employed by even the untrained saboteur because the means are almost always available and almost all targets can be destroyed by fire. In addition, fire is a natural hazard making it easier for the saboteur to camouflage his actions. The means of starting a fire are simple and, once the saboteur succeeds in igniting combustible material, time will dictate the amount of destruction achieved.

a. Origin. Fires may be classified as natural or deliberate.

(1) Natural fires include accidental fires as well as those caused by spontaneous combustion, lightning, electricity, and by sparks from other fires.

(2) Deliberate fires started by saboteurs, disgruntled employees, or people with other personal motives are often disguised as natural fires.

b. Materials. A saboteur may use the inherent combustible material of the target, or available within the target, ignited by a simple device, or he may use specifically prepared chemicals known as "hot incendiaries." When using "hot incendiaries" the saboteur usually prefers to select those meeting the following four requirements:

(1) Burn with an intense heat.
(2) Be easy to ignite.
(3) Be difficult to extinguish.
(4) Burn without leaving a residue or at least alter the external appearance of evidence at the scene of the fire.

c. Components. Incendiary devices, as well as explosives, used by a saboteur usually include three basic components.

(1) A delay mechanism provides sufficient time for the safe withdrawal of the agent who places the device, provides a time discrepancy for the establishment of an alibi, and insures the ignition or detonation of the device at the most advantageous time.

(2) An initiator insures the complete and efficient initiation of the main charge.

(3) The main charge contains sufficient incendiary or explosive material to ignite or demolish the target.

d. Simple Devices. Simple devices are those requiring little or no preparation and using materials readily available to the saboteur. Their use may be preplanned or they may be used when taking advantage of a sabotage target of opportunity. An example would be a cigarette and match folder utilized by inserting the unlighted end of the cigarette into a row of match heads in the folder. The folder would then be placed on the combustible material.

e. "Hot" Devices. If the simpler devices are not sufficiently effective to accomplish destruction of a target, the saboteur may use so-called "hot" incendiaries. A few examples are as follows:

(1) A mixture of three parts potassium chlorate and one part sugar by volume will burn at a very high temperature.

(2) Impregnating a piece of paper with white phosphorus is another effective means of making a "hot" incendiary. The impregnated paper is carried in a vial filled with water; phosphorus will not burn in water, but will ignite when it dries.

(3) Another combination is sodium and calcium carbide capsules. Sodium is placed in one gelatine capsule and a quantity of calcium carbide is placed in another and dropped into water near combustible materials. When the capsules dissolve, the sodium will ignite on the water's surface and, in turn, ignite the acetylene gas produced by calcium carbide and water. The resulting acetylene flame will ignite any nearby combustible material.

(4) Thermite, which burns at approximately 5,000° Fahrenheit and is hot enough to melt iron and steel, is made by mixing one part of aluminum powder and three parts iron oxide by volume. As thermite is difficult to extinguish, easily obtained, and produces such intense heat, it provides the type of an incendiary desired by the saboteur. However, it is difficult to ignite and leaves a residue.

f. Reference. Additional details regarding incendiary sabotage may be found in FM 19-30.

4-6. (U) Explosive Sabotage

Explosives include any chemical compounds or mechanical mixtures that, triggered by heat or shock, undergo sudden chemical change (decomposition) liberating, at high speed, heat and gas which cause tremendous pressures.

a. Employment. Explosives are employed against targets that resist destruction by other means, when destruction must be accomplished instantaneously, or when targets are of such a nature that destruction requires a shearing or shattering force. They may also be used to kill, maim, or instill fear. The use of explosives has many disadvantages and problems such as introducing the material into the target area, the need for technical or specialized training in their employment, the almost certain investigation resulting from their use, and the consequent tightening of security.

b. Classification of Explosives. Explosives are classified according to rates of decomposition as high and low explosives. A high explosive is one in which chemical decomposition occurs within an extremely short period of time; it is said to detonate. Low explosives are those in which the decomposition takes place as rapid burning; they are said to deflagrate. Explosives are also classified according to their inherent sensitivity. An insensitive explosive is one which requires only normal care in handling or storing. A sensitive explosive must be given special care in handling, storage, or use. Both high and low explosives may be either sensitive or insensitive.

c. Common Types. Explosive materials exist in different physical states and forms. Nitroglycerine is a liquid high explosive, which is very sensitive to shock. Trinitrotoluene (TNT) is a high velocity, insensitive explosive either in block form or granulated. Nitrostarch is a high velocity, insensitive explosive and has the appearance of ordinary powdered starch. Picric acid is a very powerful high velocity, insensitive explosive and is a lemon-yellow crystalline solid. Plastic explosives, such as Composition C-series which have an appearance similar to that of putty, are the ideal all-around sabotage material. Black powder is a low explosive with extreme sensitivity to heat and friction. Nipolit is an insensitive high explosive, and is a plastic which can be pressed into any desired shape, machined or cast, or formed into a one-piece bomb without casting. Additional details on explosive sabotage methods are included in FM 19-30.

4-7. (U) Mechanical Sabotage

a. Most acts of physical sabotage which are not committed by means of explosive or incendiary materials fall within the category of mechanical sabotage. This type of sabotage is one of the most difficult to prevent and the easiest to perpetrate. Mechanical sabotage is used in military operations, but most attacks are directed against transportation and industrial facilities.

b. Mechanical sabotage can be grouped into the following basic classifications, a detailed discussion of which is found in FM 19-30.

(1) *Breakage* can be directed against delicate equipment and machinery.

(2) *Abrasives* can be introduced into lubricants and fuels to cause undue wear in motors, generators, or moving parts.

(3) *Acts of omission* are those perpetrated through willful failure to act, thereby causing damage through neglect.

(4) *Substitution* is performed by replacing good with faulty materials, changing direction of shipments, or altering important points of information.

(5) *Contamination* is the introduction of substances into materials for the purpose of rendering the materials impure or injurious. A relatively new process of contamination is metal embrittlement. Embrittlement occurs when a prepared formula is placed or rubbed on the ferrous or nonferrous metal parts of the target item. When the metal part is stressed under tension—usually by mechanical means—the pores in the metal are temporarily opened. The formula then seeps into the pores and begins a rapid disintegration of the internal structure of the metal, resulting in extensive cracking and eventual total breakage of the item.

4-8. (U) Countersabotage Measures

That part of the counterintelligence mission which directs "the detection, prevention, or neutralization" of sabotage requires a comprehensive program including defensive measures and aggressive offensive action.

a. Detection of sabotage depends on thorough investigation of individual and incident complaint cases in which sabotage is alleged or suspected.

b. Prevention of sabotage is achieved through rigorous application of personnel security procedures, and establishment and enforcement of high standards of installation security.

c. Neutralization of the saboteur or sabotage organization before sabotage is attempted is the most difficult part of countersabotage operations and depends on penetration of sabotage, partisan, or other dissident groups to determine sabotage plans and identify saboteurs, methods of operations, and specific targets. No single measure or type of activity will provide adequate protection from the threat of sabotage.

Section II. COUNTERINTELLIGENCE OPERATIONS

7-2. (U) General

Standard counterintelligence practices and procedures as set forth in FM 30-17 are applicable in conducting counterintelligence activities for stability operations. Standard practices and procedures differ only in degree and emphasis. Counterintelligence aspects of stability special operations are discussed in this section.

CHAPTER 8

TACTICAL COUNTERINTELLIGENCE—DATA BASE

Section I. FILES, INDICES AND ANALYSES

8-1. (U) General

a. Effective counterintelligence operations are frequently dependent on the quality and completeness of files, indices, and the analyses of these files and indices. This chapter discusses files, indices and analyses at the tactical level during an insurgency; however, with slight modification, this information is applicable at all levels of command, and in all intensities of warfare.

b. Files and indices, after proper analysis, should yield insurgent indicators (FM 30-5 and FM 30-31), and generate a useful data base from which target recommendations, populace and resources control measures, base camp security recommendations, and counterintelligence special operations, can be made.

c. Counterintelligence files provide the counterintelligence element with an expedient reference data base from which can be drawn accurate, timely information for use in both short- and long-range counterintelligence operations. Additionally, these files will provide a measure of continuity of operations and eliminate the possibility that element personnel will waste time and effort on activities and methods attempted or rejected during previous operations. They will also provide a means for quickly orienting newly assigned personnel. One warning, however, must be borne constantly in mind. Too much information is often as confusing as too little. Good files are continuously screened in order to eliminate obsolete or irrelevant material.

d. From this data base, the counterintelligence element can recommend tactical interception, cordon and search operations, raids and searches, population and resources control measures, border security measures, and other tactical operations to the commander.

8-3. (U) Cross-Referencing

Figure 8-19 graphically shows the cross-referencing of files. If the information contained in a file cannot be found, then the file is worthless. This figure only suggests a cross-referencing system for each echelon and each combat environment must devise its own system to fit its own needs.

8-4. (U) Use of Files

Counterintelligence files have many varied uses as depicted in figure 8-20. Basically, these files are an aid to further collection and/or to tactical exploitation for support of the tactical commander and in support of the unit's mission. To fully illustrate the use of the foregoing files, the following examples are furnished:

a. Enemy Boundaries. Insurgents frequently have different political and jurisdictional boundaries than the host government. A data base that does not indicate these different boundaries will be incomplete thus allowing insurgent exploitation of the boundaries, and a distortion of the insurgent infrastructure is created. One advantage to the insurgent could be tactical if the host government employs regional military forces in fixed AOs. For example, the host government has two subdivisions A and B as depicted in figure 8-21 while the insurgent subdivision C overlaps the two. In this instance, the insurgents can attack a target in subdivision B and move rapidly into subdivision A while the subdivision troops in B will be forced to stop at boundary AB. The insurgents, since they are still in their own subdivision, will be near familiar caches and rest areas. The solution would be close cooperation between the two subdivisions A and B as long as the insurgent chooses to maintain subdivision C. In addition, the insurgent's subdivisional boundaries reflect his needs and capabilities, and where he feels strongest. This information could be vital in an analysis of administrative and pacification roles to be taken by the host government.

b. Enemy Control. The host government's presence, or lack of it, is an indicator as to how much control the host government exercises in an area. The absence of host government tax offices, schools, police departments, hospitals, and elections in areas is indicative of insurgent control. This information can be obtained from a political SITMAP where insurgent and host country agencies are map plotted.

c. Enemy Initiated Incidents. The political SIT MAP can form a nucleus for analysis of enemy initiated incidents. Each abduction, bombing, assassination or other such action should be plotted. The analyst, however, should not jump to conclusions but should analyze such activity carefully. The lack of such activity could mean the insurgent is strongly in control or it could mean he has no control. Conversely, a high incident rate may indicate that the

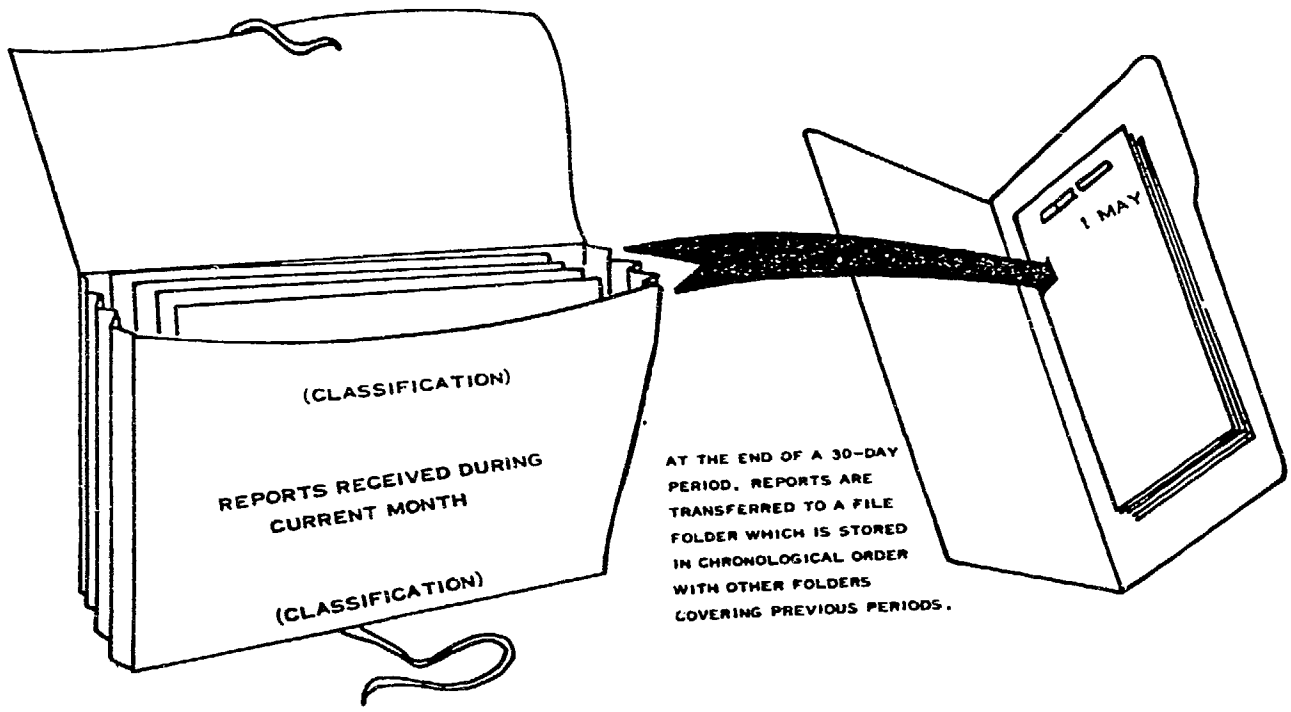


Figure 8-17 (U). Incident files (U).

~~CONFIDENTIAL~~

FM 30-17A

(CLASSIFICATION)

DAILY STAFF JOURNAL OR DUTY OFFICER'S LOG
(AR 220-346 & FM 101-5)

PAGE NO: 2 | NO OF PAGES: 2

ORGANIZATION OR INSTALLATION	LOCATION	PERIOD COVERED FROM HOUR	FROM DATE	TO HOUR	TO DATE
CI SECTION, 2332 MI DET 20TH DIVISION	PHILGERIA	0001	18 May 84	2400	18 May 84

ITEM NO	TIME IN	TIME OUT	INCIDENTS, MESSAGES, ORDERS, ETC.	ACTION TAKEN	INL
26	2330	2035	FM Tm A via radio: Radio station vic UTM	G2, CA Notified.	LAV
			365402 searched. 12 lbs docts uncovered.		
			Four guards posted.		
27	2340	2045	FM Div G2 via L/L: S2, 1st Bde reported arm-	Tm D instr to	LAV
			ed civ captured en route to PW cage.	proceed to PWC.	
28	2355	2400	FM Tm B via radio: Circle Trigon Party	Tm F ordered to	LAV
			official disclosed loc of concealed enemy	site to remove	
			records in cave at UTM 370621.	docts to CP &	
				cont intg of CIP	
				official.	

TYPED NAME AND GRADE OF OFFICER OR OFFICIAL ON DUTY: Lucius A. Valliant, S/A, 2332 MI Det

SIGNATURE: Lucius A. Valliant

DA FORM 1 NOV 62 1594 — PREVIOUS EDITION OF THIS FORM IS OBSOLETE. — U.S. GOVERNMENT PRINTING OFFICE 1967 O—654154

(CLASSIFICATION)

Figure 8-18 (U). CI journal (U).

~~CONFIDENTIAL~~

insurgent is employing terrorism to consolidate his control over contested areas. Basically, incidents do have a meaning. The key is interpretation.

d. Organizational Files. Organizational files, to include line and block charts, are useful analytical tools for establishing enemy subordination and strength. A well-developed, complicated line and block chart allows the analyst to draw certain conclusions about the insurgent, for example, his organizational and numerical strength, particularly in areas of low military and political activity. New organizations might reflect a change in mission or additional missions assigned to that subdivision. Deletions of old organizations, and consolidations of existing organizations could mean the insurgent is being hurt, either in this subdivision or in others, or it could mean he is streamlining these organizations for a new mission. By also analyzing who is subordinate to whom, it will be easier to establish priorities for targeting against the organization or individuals within it.

e. Other Uses. Money and food are important to the insurgent. Map plots of taxation points or food drops may indicate exploitable patterns of insurgent activity. The use of the data base, therefore, is limited only by the person making the analysis of the information contained therein.

Section II. PATTERN ANALYSIS

8-6. (U) General

Because human beings have certain needs and habits, the insurgent's activities, movement and locations, may be analyzed through pattern analysis. Counter-intelligence personnel should be aware of these methods in case of employment in support of stability operations.

8-7. (U) Area of Operations

An analysis of the insurgent should first begin with the "area-of-operation" study. This study should yield descriptive facts about the area, a discussion on how they influence certain factors selected for their importance in developing courses of actions, and conslusions on how the influenced factors affect possible courses of action.

8-9. (U) Terrain Analysis

In effect, the above analysis leads into a parallel analysis which can be furnished to the tactical commander. Terrain needs to be factually described for its effect on insurgent and on counterinsurgent. If certain terrain features are best suited for insurgent basing areas, then the counterinsurgent should consider all terrain of this type as key terrain. The same principle applies to avenues of approach which are logically, in an insurgency, avenues of movement since an insurgent band tends to retrace its previous movement.

698-493 O - 71 - 6

APPENDIX A

REFERENCES

AR 380-series	Military Security.
AR 381-series	Military Intelligence.
AR 405–10	Acquisition of Real Property and Interest Therein.
AR 710–2	Materiel Management for Using Units, Support Units, and Installations.
DA Pam 310-series	Indices, as appropriate.
DA Pam 381-series	Intelligence, Security, and Related Subjects.
(S) DIAI 58–19	Defense Intelligence Agency Instructions (U).
(S) DIAI 58–21	Defense Intelligence Agency Instructions, Intelligence Acquisition (ISR) (U).
(S) DIAM 58–1	Defense Intelligence Acquisition Manual (U).
(S) DIAM 58–11	Defense Human Resources Intelligence Collection Management Manual (U). Vol I, Human Resources Collection System Management. Vol II, Controlled HUMINT Collection Operational Planning and Tradecraft.
FM 19–30	Physical Security.
FM 19–40	Enemy Prisoners of War and Civilian Internees.
FM 21–76	Survival, Evasion, and Escape.
FM 30–15	Intelligence Interrogation.
FM 30–16	Technical Intelligence.
FM 30–17	Counterintelligence Operations.
(S) FM 30–18	Intelligence Collection Operations Intelligence Corps, WSA (U).
FM 30–31	Stability Operations-Intelligence.
FM 31–73	Advisor Handbook for Stability Operations.
(C) FM 32–5	Signal Security (SIGSEC) (U).
FM 33–1	Psychological Operations—US Army Doctrine.
FM 100-series	Field Service Regulations.
FM 101-series	Staff Officers.
TB (PMG series)	Provost Marshal General.
TC 3–16	Employment of Riot Control Agents, Flame, Smoke, Plant Agents, and Personnel Detectors in Counterguerrilla Operations.
TOE 30-series	Military Intelligence.

Note. For additional references, see FM 30–17.

APPENDIX B (U)(C)

HOSTILE ESPIONAGE ORGANIZATION AND METHODS OF OPERATION

B-1. Introduction

a. (U) Basic methods of espionage have not varied significantly in the past except as technological developments have permitted the sophistication and modification of these methods. Regardless of the sponsoring country, certain factors or principles have contributed to successful espionage operations. The purpose of this appendix is to amplify the doctrine on espionage contained in chapter 2 by presenting additional information on espionage organizations and fundamental methods of operation.

c. (U) Countries with many years of experience in worldwide espionage have achieved a high degree of professionalism in their intelligence personnel. Staff and operational personnel are carefully selected after thorough investigation with maximum emphasis on political loyalty. Intelligence may be a lifetime profession, barring purges, and there is a great deal of specialization. Intelligence personnel are well acquainted with the language, history, economics, and politics of their target countries. Frequently, they spend time in the target country for area familiarization prior to engaging in espionage operations.

e. (U) United States constitutional liberties have been studied in detail, and hostile intelligence organizations take full advantage of our freedoms of speech, press, and religion; the right of assembly and meetings, democratic elections, the legal existence of more than one political party, our judicial system, our self-chosen pursuits of education and professions, the freedom of internal and external travel, and the absence of censorship of communications.

B-2. Operational Controls

(U) In operations in the field, three fundamental operational control procedures are usually exercised by hostile intelligence organizations. These controls emphasize the concern for operational security.

(c) (U) The legal agency can also participate, to a large extent, in overt collection. It has been stated by several defectors from hostile intelligence that as high as 90 percent of their intelligence requirements against the US can be fulfilled through the collection of material openly available.

B-3. Types of Operations

(U) Hostile intelligence operations abroad may be referred to as either legal or illegal. This distinction has nothing to do with the legality of espionage; rather it refers to the status of the personnel involved in such operations.

(1) (U) The legal operation makes use of legal representations such as an embassy, consulate, trade or cultural mission, exchange group, or economic organization as cover for the hostile intelligence personnel. As a member of such a legal representation, one is in the target country with official status, sanctioned by the host government.

(a) (U) In a legal operation, hostile intelligence personnel may enjoy the privilege of diplomatic immunity; they are not subject to search, arrest, or prosecution for their unlawful activities. At best, they can be declared *persona non grata* and asked to leave the country.

(b) (U) The legal operation, particularly when controlled from diplomatic representations, has relatively secure communications with the headquarters in the home country through use of the diplomatic pouch. Communications is a prime problem for agents and this method offers a good solution.

B-4. Types of Agents and Agent Systems

(U) In conducting espionage operations, hostile intelligence uses several types of agents and agent systems:

a. (U) The individual agent system involves the intelligence collection efforts of one person. The intelligence collector operates alone, with direct clandestine communication with intelligence in the home country (via radio, courier, or personal contact). He may have support agents such as radio operators or courier system, or both; however, only one person does the collecting. An individual agent may be any one of the several categories of agents, as follows:

(1) (U) *Penetration agents.* These agents have direct access to information of a military, political, economic, scientific, or counterintelligence nature.

(2) (U) *Mass recruited agents.* Mass recruited agents are low-level, poorly trained agents who are infiltrated into target countries in large numbers whenever favorable opportunities exist. They are infiltrated among refugee streams, repatriated prisoners of war, displaced persons, and linecrossers. They are assigned low-level missions, such as the collection of military unit identification, movements of military equipment and weapons, and troop maneuver activities. The hostile intelligence services have little difficulty in recruiting them. The compromise of a few does not really constitute much of an operational loss since quantity, rather than quality, is a major consideration in these operations.

(3) (U) *Confusion and provocation agents.* Some confusion agents are instructed to fabricate long and detailed stories of contact with hostile intelligence. The hope is to lure target country counterintelligence into recruiting these agents or dissipating its efforts in useless investigation. Others may carry fabricated documents containing seemingly important data concerning the home country for the purpose of deceiving and misdirecting counterintelligence. Provocation agents are used to provoke target country counterintelligence agencies into some course of action which will be to their disadvantage and to the advantage of the sponsoring country. For example, an agent may be instructed to contact a target country intelligence agency and denounce a public official as being an informant of hostile intelligence. A false denunciation of this type could result in lengthy investigation of the official concerned and possibly organizational upheavals.

(4) (U) *Sleeper agents.* Sleeper agents may be infiltrated into the target country or recruited from among local residents. They remain inactive until the sponsoring intelligence service has a specific mission for them to perform. Sleeper agents, for the greater part, cost little or nothing, and some have the potential of developing into high-level, well-concealed agents.

B-5. Multiple Coverage

a. (U) More than one espionage system from the same or different intelligence agencies may be used concurrently to operate against the same target or project. They may operate independently of each other and may not know of each other's existence.

b. (U) Multiple coverage increases the possibility that the desired information will be obtained. Furthermore, information obtained from the different nets can be compared in order to submit a more complete and accurate evaluation, as well as to reorient the effort when necessary.

B-6. Agent Recruitment

(U) Espionage practices normally include at least a three-phase recruitment. These phases are spotting, analysis or study, and the approach.

a. (U) Hostile intelligence must locate individuals who can be induced or coerced into accepting recruitment. Emphasis is naturally placed on persons who have access to information sought, or on persons who might later be inserted into positions of access. Higher-level professional persons are sought—government officials, scientists, managers, educators, military officers, medical doctors, and others. However, the unschooled, the semiskilled, and the lower military ranks, e.g., messengers, communication center personnel, are lucrative sources and also serve useful purposes as espionage agents. A secretary, typist, or a message center clerk may have access to highly sensitive information which would make him an extremely valuable agent.

B-7. Agent Motivation

(U) There are many motivations used in recruiting agents. Of these, three are exploited most frequently by hostile intelligence agencies:

a. (U) *Ideology.* Preference is given to the ideological recruit; that is, the one favorably disposed toward home country or its national theories. This type of person generally is the most reliable, for he works with political conviction, zeal, perseverance, and complete adherence to policies and instructions; he is frequently willing to make many personal sacrifices.

b. (U) *Remuneration.* Hostile intelligence has recruited many individuals on the basis of mercenary tendencies. Some mercenaries offer to sell information to the hostile service, and others are recruited after having been spotted by hostile intelligence representatives in the target country.

(1) (U) "Walk-ins" may have large gambling debts; they may have wild spending proclivities; or they may be motivated simply by greed. Generally, their intentions are to sell information to the hostile intelligence service or to any buyer on a short-term basis. Hostile intelligence may be quick to take advantage of these exploitation opportunities; and as soon as possible they develop leverage factors to force the informants' continued cooperation.

(2) (U) Hostile intelligence is continuously on the lookout for individuals with financial difficulties or other personal problems. Excessive gamblers, alcoholics, and irresponsible spenders in the Army are among the favored recruitment targets. Attractive females are often used to induce soldiers to spend money freely and excessively. Sometimes females are successful in persuading the soldiers to provide information for money, an "easy" means for them to continue their indulgences. Initial requests are sometimes camouflaged by false claims that the desired information is for some national cause, research institute, or friendly country. The innocent requests then develop into demands, with the revelation that hostile intelligence has been the recipient of information already provided.

c. (U) *Pressure.* The instances in which hostile intelligence services have recruited by pressure tactics are innumerable. Despite the fact that many individuals have reported pressure recruitment approaches and actual involvement in espionage, pressure tactics have been used with a great deal of success. The tactics may take numerous forms, and their effectiveness depends upon the extent to which various types of acts have been tolerated in the target countries.

(1) (U) *Threats to expose past or current criminal activities which have not come to the attention of employers or law enforcement agencies.* The criminal acts may involve anything from black-marketing to theft, smuggling, extortion, dope peddling, sexual crimes, and even murder. In some cases, hostile intelligence has induced individuals to commit or participate in criminal acts, the sole purpose being to develop pressure points which can be applied in forcing them to engage in espionage.

(2) (U) *Exploitation of character weaknesses and indiscretions.* These frailties might involve alcoholism, drug addiction, adultery, or sexual perversion. Female agents are used to lure soldiers into illicit sexual affairs, and homosexual agents are placed in contact with Army homosexuals. The soldiers are then confronted with photographs of the acts, with threats to send prints to wives, superior officers, or government officials, unless they agree to cooperate. Because of the many control problems presented by drug users, hostile intelligence services are not expected to exploit a drug addict except on a one-time-basis proposition.

(3) (U) *Exploitation of prisoners and prisoners of war.* There have been cases where political prisoners were offered early release, provided they sign agreements to work as agents. The same is true of prisoners of war, who are offered early repatriation or who are threatened with nonrepatriation, the condition being that they work as agents after release. Another technique is to threaten the prisoner of war with torture or death unless they become informers. Once they cooperate, levers can be applied to force their cooperation after repatriation.

(4) (U) *Exploitation of family ties.* Active agents are persuaded or pressured into recruiting their close relatives. This can be done with considerable impunity, because the relatives are often reluctant to expose the recruiter-relative to the authorities. Many agents have been recruited through threats to first degree relatives living in the home country of the hostile intelligence service. Threats may entail confiscation of property, imprisonment, incarceration in slave labor camps, torture, and even death. A variation is the promise to allow relatives to emigrate to the West, provided that the subject agrees to cooperate. Pressure recruitments through

relatives frequently are accompanied by financial inducements, either directly to the subject or to relatives kept as hostages.

B-8. Cover

a. (U) As may be assumed, hostile intelligence spends a great deal of time planning and developing cover for espionage agents. In the "legal" operation, the agency may spend several months or even a year learning his job to support his cover story in the West. In the "illegal" operation, cover must be constructed to permit the agent to disappear into the population of the target country. To this end, the tremendous files available at the headquarters provide the necessary background information.

b. (U) Generally, hostile intelligence categorizes cover as either "natural" or "artificial."

(1) (U) Natural cover takes the form of legal residence or legal entry into a country, the use of true names in most instances, authentic documentation, and a normal or legal occupation. The best examples of agents using natural cover are natives of a target country with legitimate occupations and no connections whatsoever with the home country. Other examples are persons recruited from among repatriates and refugees, and hostile intelligence officers serving aboard in diplomatic and other official representations.

(2) (U) Artificial cover involves the fabrication of an agent's background and status, and falsification of documents, passports, and other identification documents in such a manner as to match the agent's fabricated background and cover story. Sometimes certain parts of the cover story must be backstopped so that if officials check parts of the story against official records, the records will support and verify the false parts of the cover story. Home country nationality and all connections with it are concealed.

c. (U) Obviously, artificial cover is much more difficult to establish and maintain than natural cover. A great deal of planning and preparation must precede the use of artificial cover, taking into consideration the agent's linguistic ability, accent, habits, clothing, education, professional training, and familiarity with the customs and characteristics of pertinent geographic areas. The training and preparation for an assignment may take years.

B-9. Training

(U) Agent training begins with the recruitment. Hostile intelligence gives agents two types of training—political and technical. The training usually continues as long as the agent is active.

a. (U) *Political Indoctrination.* Agents who are trained in the home country or who meet their handlers there, regardless of their motivations, are generally subjected to a great deal of political indoctrination. Indoctrination is administered at meetings between the handler and the agent, and it comprises a large portion of the curriculum if the agent attends an intelligence or espionage school. The national theories are expounded upon, as well as the advancements of the home country. At the same time, the United States is painted as a decadent, corrupt, and warmongering capitalistic society. The objective is to convert the agent completely, thereby strengthening his political reliability and ideological convictions. Agents met in the West generally receive a minimum of political indoctrination in order to keep meetings between agents and agent handlers as brief as possible.

b. (U) *Technical Training.*

(1) (U) Cadre workers (staff officer agents) of hostile intelligence are well qualified for espionage work, and their intelligence training is specific and detailed. Espionage agents in the field are predominantly of a nationality other than the home country. These agents are given espionage training to the extent necessary to complete their assigned missions, to include contact and identification arrangements, detection of surveillance, selection and use of letter drops, concealment of information for transmittal, and perhaps simple techniques of photography, codes, and secret writing. Higher level agents are given additional and more refined training in espionage tradescraft, which might include instruction in advanced photography, microphotography, intricate codes and secret writing systems, and clandestine radio assembly and operation. Where necessary, some are also trained in an occupation which will serve as effective cover and facilitate the development of natural access to the target.

(2) (U) Most agents receive espionage training from their handlers rather than from formal intelligence schools. A few highly competent agents are sent to home country headquarters for more specialized and formal intelligence training when such training is deemed essential. A few of these individuals may eventually reach the stature of "illegal" resident net directors abroad. These agents, of course, must be of demonstrated reliability and motivation.

B-10. Operations Security

(U) Successful espionage requires a high level of operations security. In no other aspect of operations is this concern for security more apparent than in the conduct of meetings. Certain techniques have come to be standard procedure for hostile intelligence in this concern for security.

B-11. Communications

(U) Hostile intelligence, in its worldwide operations, must rely on sound, secure communications. Generally, couriers are preferred as the most secure and having the capability of transmitting the largest amount of material. The next preference is radio, the fastest but least secure method. It appears that hostile intelligence may reserve radio for imminent reporting and wartime operations, although there is evidence that agents in the US may be able to use offshore trawlers or submarines as relay stations. In some countries, commercial cable lines are used to exchange enciphered messages.

a. (U) *Courier Communications.*

(1) (U) Widespread use is made of couriers who enter and leave target countries, both legally and illegally. Examples of legal courier systems are embassies, consulates, and military attaches who make extensive use of diplomatic pouch for espionage communications. Illegal courier systems involve the use of illegal and nondiplomatic legal travelers. Examples are illegal border crossers, seamen, tourists, and intelligence officers assigned to cultural exchange groups and certain international trade organizations.

(2) (U) Bulky documents are usually reduced to microfilm, which is carried through courier systems. Often, the films are carried undeveloped so that in the imminence of search or arrest, the courier can expose them to light and destroy the evidence of espionage. Even when the diplomatic pouch is used, information is transmitted on undeveloped microfilm.

(3) (U) In some cases, *soft film* is used. The hard acetate backing is removed from film negatives, making them thin and pliable so that they can be rolled up and hidden in small concealment devices. Still another technique is the use of microdots. This technique consists of the reduction of a film negative to the size of a pinhead, which can be concealed in any one of numerous places on a person's body, in his clothing, or in luggage or other articles which are carried. Unless a person is suspected of carrying microdots and is subjected to a meticulous search, their presence is almost impossible to detect.

(4) (U) If the information is not photographed, it can be written in code or in secret writing, or a combination of both. In view of their vulnerability to arrest, couriers generally are not permitted to know the code and secret writing systems used in the communications they carry. Courier communications are used most extensively and with greatest effectiveness during peacetime, because it is then that international travel and border restrictions are at a minimum.

(5) The transmission of information by courier, although the most secure, presents a problem for the courier. Therefore, hostile intelligence agencies use concealment devices of numerous types to transmit and store espionage messages. These devices are such articles as hollowed-out coins, buttons, screws, bolts, cufflinks, rings, pencils, secret compartments in suitcases, briefcases, handbags, toilet articles, shoes and others. These devices make it easier for espionage operatives to conceal microdots, microfilm, and thin sheaves of paper. Considerable effort and money is devoted to development and manufacture of such devices.

(6) In addition to the transmission information, the espionage agent or even the director may have need for a storage place for information or equipment. Such caches receive considerable attention from hostile intelligence.

b. Mail Communications.

(1) Information is transmitted through the mails, making use of codes, secret writing, simple coded phrases, and microdots. Code messages are usually reduced to secret writing, and coded phrases are used throughout the visible text of the letter to transmit short messages. Microdots can be concealed on typewritten texts of a letter, under the flap or postage stamp, or in the case of post cards between the fibers or on the face of the card.

(2) Espionage communications are often transmitted through neutral or third countries. Circuitous routing slows down communications, but it increases the effectiveness of security. Espionage communications through international mails are vulnerable to detection during wartime when censorship is widely imposed.

c. Radio Communications.

(1) Radios are used *overtly* by embassies and consulates. Enciphered messages are transmitted and received over high-powered wireless radio sets which are legally authorized.

(2) Two types of *clandestine* radio communication which are commonly used by hostile intelligence are the one-way system and the two-way system. When the one-way system is used, coded messages are transmitted over powerful commercial radio networks from the home country, generally by shortwave. Using an ordinary home radio set with a shortwave band, the agent in the target country listens to transmissions at designated times, transcribes the messages intended for him and deciphers them. A disadvantage of this system is that the agent does not have a rapid method of communicating with the intelligence service in the home country. When the two-way system is used the agent has a transceiver radio, compact in size and designed for clandestine operations.

(3) Cipher systems are used with both radio systems to translate open text material into groups of usually five numbers. In deciphering the messages, an agent uses a code devised for his exclusive use. Some cipher systems are based on a one-time-pad system. The sender and recipient both have identical code pads. The sender uses one or more sheets for a message, and the recipient uses the corresponding identical sheets to decipher the message. Both parties then destroy the used sheets and take up the next one. If the code used in any one message is broken, succeeding messages cannot be deciphered.

(4) Clandestine radio communications are vulnerable to interception and direction-finding operations, especially when transmissions are lengthy. These hazards have been partially overcome by the development of magnetic tape recordings. The entire message is recorded on magnetic tape and then transmitted at high speed (burst transmission) so that the entire length of time the transmission is on the air is reduced to seconds.

(5) The use of clandestine radio remains largely a device for wartime operations for use by stay-behind nets in enemy rear areas since other means of communication are generally more secure during peacetime. In wartime, radio is often the most practical method of communication. It should be borne in mind that hostile intelligence agencies establish numerous clandestine radio communication systems in target countries so that they will be available for use in the event of war.

B-12. Finances

a. Hostile intelligence finances its espionage operations, wherever possible, in the currency of the area of operation, so that agents will not be picked up with large amounts of currency foreign to the countries in which they are operating.

b. Almost unlimited funds for espionage operations may come from the national budget of the home country of the intelligence service. Other sources of funds are businesses and cover organizations established for that purpose. Some agents are directed to engage in illegal activities to raise funds and to obtain local currencies by such means as extortion, blackmarket activity, and counterfeiting. Some agents are given saleable articles such as gold, jewelry, narcotics, and scarce medicines for conversion to money. Others are trained in professions which will enable self-support in the target area and add weight to the cover story.

c. Funds are transmitted into target countries and to espionage agents by diplomatic pouch, by other official representatives in the target country, by clandestine couriers such as merchant seamen, and by agents themselves when entering target countries.

Through international currency transactions, bank balances may be established in the target country in the name of a support agent. Checks are then sent, as required, to the espionage agent under some pretext.

B-13. Disposition of Agents

(U) Hostile intelligence apparently makes some distinction between staff officers and agents in considering dispositions. Reported disposition techniques include the following:

(1) (U) On learning that agents were compromised and in danger of arrest, hostile intelligence warned them to go into hiding or to make their way to the home or friendly country. This resulted in the termination of their services, or their identities and covers were changed for operation elsewhere in the target country.

(2) (U) When hostile intelligence learned that agents were intelligence swindlers or had been doubled by target country counterintelligence, it directed their return when possible to a friendly country on some apparently innocent pretext. Swindlers frequently have been imprisoned. Doubled agents have been imprisoned or sent to slave labor camps, or they have been redoubled.

(3) (U) Intelligence staff officers whose missions were completed in a target country were recalled to the home country, and a number of them later appeared in the same or different countries.

(4) (U) Resident type espionage agents whose specific missions were completed were transferred to other targets in the same country, or they temporarily became dormant.

(5) (U) In cases where intelligence staff officers defected to the West, efforts were made to locate them and persuade them to return to the home country with promises that they would not be prosecuted. The fate for such individuals was death, or at best, life imprisonment. When hostile intelligence had reason to believe that staff officers were contemplating defection, they were directed to return immediately to the home country or they were taken into physical custody and forcibly returned. These individuals were never heard of again.

5. (U) All the major espionage services operate in a similar manner with deviations to meet local conditions. In attempting to counter the activities of hostile intelligence services, it is wise to remember that most of the key intelligence officers are well trained and experienced.

6. (U) In conclusion, it should be noted that, even though the organization and methods of operation are extremely professional and well conceived, men are required to make these organizations and techniques effective. This is the basic weakness of all espionage—man.

~~CONFIDENTIAL~~

Page 1 of 3 Pages

DEPARTMENT OF DEFENSE BIOGRAPHIC REPORT

GENERAL INFORMATION

1. COUNTRY
2. DATE OF INFORMATION (Yr, mo, day)
3. DATE OF REPORT (Yr, mo, day)
4. NAME
   a. FULL NAME (Give full name in Roman letters, in natural order, and with natural capitalization. Underline surname, or, if known by name(s) other than surname, underline name. Give phonetic pronunciation of name as appropriate).
   b. NAME OR NAMES BY WHICH INDIVIDUAL PREFERS TO BE ADDRESSED
      (1) IN OFFICIAL CORRESPONDENCE:
      (2) ORALLY AT OFFICIAL GATHERINGS:
   c. FULL NAME IN NATIVE ALPHABET
   d. VARIANTS, ALIASES, OR NICKNAMES
5. POSITION
   a. PRESENT POSITION
   b. DATE ASSUMED POSITION (Year, month, day)
   c. RANK/TITLE (In English and Native language)
   d. DATE OF RANK (Yr, mo, day)
   e. SERVICE
   f. BRANCH OF SERVICE
6. DATE AND PLACE OF BIRTH (Town, State, Province, Country)
   g. SEX
10. PRESENT ADDRESS (Including unit location if applicable)
    TELEPHONE NO
11. NATIONALITY
12. RACE
13. PHOTO SUBMITTED ☐ YES ☐ NO
14. CITIZENSHIP (Indicate dual citizenship where applicable)
15. RELIGION ☐ PRACTICING ☐ NONPRACTICING
16. TITLES AND HONORIFICS (Prince, Doctor, Military, etc.)
17. MARITAL STATUS ☐ MARRIED ☐ SINGLE ☐ DIVORCED ☐ WIDOWED

PHYSICAL DESCRIPTION

18. AGE
19. BEARD ☐ YES ☐ NO MUSTACHE ☐ YES ☐ NO
20. TEETH (Natural) ☐ YES ☐ NO
21. PROMINENT OR UNUSUAL FEATURES (Moles, scars, birthmarks, etc.)
22. COLOR EYES
23. COLOR HAIR
24. BALD ☐ YES ☐ NO
25. HEIGHT
26. WEIGHT
27. BUILD (Small, medium, large)
28. POSTURE
29. ☐ RIGHT HANDED ☐ LEFT HANDED
30. PHYSICAL DEFECTS
31. GENERAL STATE OF HEALTH
32. HARD OF HEARING ☐ YES ☐ NO
33. GLASSES ☐ YES ☐ NO

PERSONAL BACKGROUND

34. CIVIL EDUCATION (List schools, location(s), major courses, degree(s), honors, and inclusive dates (Year, month, day).
35. LANGUAGE PROFICIENCY (Include dialects, degree of fluency, and ability to act as translator/interpreter).
36. TRAVEL (List countries, dates, and purpose).

SAMPLE

DD FORM 1 MAR 67 1396-1 EDITION OF 1 NOV 63 IS OBSOLETE.

Figure D-2 (U). Biographic report (U).

~~CONFIDENTIAL~~

Page 2 of 3 Pages

37. MILITARY SERVICE (a. *List military career in chronological order. Include: Military schooling, promotions, demotions, foreign service, units served with and position held; location of school or unit, retired or reserve status.)*

(b. List awards and decorations together with circumstances surrounding any unusual award/decoration.)

SAMPLE

38. EMPLOYMENT OTHER THAN MILITARY SERVICE *(List employers, positions, skills, locations, and inclusive dates (Year, month, day).*

39. MEMBERSHIP IN ORGANIZATIONS *(Professional, social, military, other, give inclusive dates (Year, month, day).*

EDITION OF 1 NOV 63, IS OBSOLETE

Figure D 2 (U). Continued (U).

~~CONFIDENTIAL~~

Page 3 of 3 Pages

40. U.S. ACQUAINTANCES AND RELATIVES *(Name, position or occupation of relatives, domicile, nature and duration of relationship. Include U.S. military or other U.S. official acquaintances/relatives under this item.)*

41. PREFERENCES *(Personal preference in food, drink, tobacco, entertainment, sports, hobbies.)*

42. PUBLISHED WORKS *(Title of article or book; if article, name of publication appearing in, date published, publisher.)*

SAMPLE

SPOUSE – FAMILY

43. FULL NAME OF SPOUSE

44. MAIDEN NAME OF SPOUSE

45. DATE *(Year, month, day)* AND PLACE OF BIRTH

46. NATIONALITY *(Indicate dual citizenship where applicable)*

47. RACE

48. RELIGION
☐ PRACTICING
☐ NONPRACTICING

49. BACKGROUND *(Education; language preference in food and drink; hobbies; preference in entertainment; special interests; professional societies.)*

50. CHILDREN *(Names, sex, ages, marital status, other items of interest such as schools, health, military service.)*

EDITION OF 1 NOV 53, IS OBSOLETE.

U. S. GOVERNMENT PRINTING OFFICE : 1957 O - 353-884

Figure D-2 (U)—Continued (U).

~~CONFIDENTIAL~~

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED

I, _____, born on _____ at _____, presently residing at _____, acknowledge that I have voluntarily cooperated with US (Army) Intelligence in a classified activity at _____ (geographic location) during the period * _____ to ** _____. I have received in full all remunerations and allowances due me. All promises made to me have been discharged and there are no other outstanding obligations of any kind due me. I have no further claim against US (Army) Intelligence or the US Government.

*Date of Recruitment or Initial Activity of Source
**Date of Termination

_____ (Witness)

_____ (Signature)

_____ (Date)

(Classified When Completed)

(For Non-US Nationals—Termination)

Figure D-9 (U). Severance statement (U).

SECURITY
CERTIFICATE

I, _____ (Name, DPOB, SSAN)

certify that I have on this date been entrusted with information concerning a sensitive classified intelligence operation/investigation, and agree to perform functions assigned in conjunction therewith. I realize that the operation/investigation is classified within the meaning of national defense security regulations and I understand the importance to national security to protect the sensitive information which I have received or may gain as a result of my activities in this project. I recognize that the Uniform Code of Military Justice and Title 18 of the United States Code apply and that I am obligated to withhold all information relating to this project from all other persons and agencies, except as may be specifically authorized by US Army Intelligence.

_____ (Date)

_____ (Signature)

_____

(Classified when completed)

(For US National Source Only, When Recruited)

Figure D-10 (U). Security certificate (U).

SECURITY

CERTIFICATE

WARNING NOTICE: SENSITIVE SOURCES AND METHODS INVOLVED

I, _____, certify that I have been informed by Mr. _____, an authorized representative of the United States Army Intelligence, that disclosure of the nature, sources, or even the existence of counterintelligence activities, to which I have become party, are not to be disclosed to any persons without the express approval of the United States Army Intelligence.

I further certify that I am aware of the provisions of AR 380-5, and that any unauthorized disclosure of the counterintelligence information discussed with me by the above-named representative of the United States Army Intelligence, will be considered a violation of AR 380-5, and will subject me to appropriate disciplinary action.

_____ (Date) _____ (Signature)

_____

(Classified When Completed)

(For US Military Source—Termination)

Figure D-11 (U). Security certificate (U).

SECURITY

CERTIFICATE

I, _____, acknowledge this date that I have voluntarily cooperate with intelligence officials in a sensitive classified security operation/investigation during the perio _____ to _____. I have received all remunerations and allowanc due me and there are no other outstanding obligations. I realize that the operation is classified within t meaning of national defense security to protect the sensitive information which I have received. I recogni that Title 18 of the United States Code applies and that I am obligated to withhold all information relating this project from all other persons and agencies and may not publicize, reveal, or infer my past participati in such operation/investigation.

_____ (Date) _____ (Signature)

_____

(Witness (Case Officer))

(Classified When Completed)

(For US National Sources—Termination)

Figure D-12 (U). Security certificate (U).

SECURITY AGREEMENT

I, _____, presently residing at, _____, have, on this date, been entrusted with information concerning a sensitive intelligence operation and have agreed to perform activity in behalf of US Army Intelligence (or US Intelligence) in conjunction therewith. I realize that the existence itself of the operation, its objectives, and any other information concerning it of which I am or may become knowledgeable, is confidential in nature and cannot be imparted to any individual except under the guidance, and upon the specific approval, of a duly identified and authorized member of US Army Intelligence (or US Intelligence). I realize that any failure on my part to maintain strict confidence concerning any and all aspects of the operation of which I am or may become knowledgeable may cause me to become liable to prosecution under provisions of * _____, and under such other laws or ordinances as may be applicable in the case.

*Insert identification of applicable section/paragraph of the legal code under which individual may be prosecuted.

_____ (Witness)

_____ (Signature)

_____ (Date)

(Classified when completed)

(For non-US nationals only, when recruited)

Figure D-13 (U). Security certificate (U).

APPENDIX E (C)

SURVEILLANCE RADIO COMMUNICATION-CODES (U)

E-3. (U) Police 10-Series

The standard police 10-series is as follows:

10-1 Receiving Poorly
10-2 Receiving Well
10-3 Stop Transmitting
10-4 OK, Message Received
10-5 Relay Message
10-6 Busy, Stand By
10-7 Out of Service, Leaving Air
10-8 In Service, Subject To Call
10-9 Repeat Message
10-10 Transmission Completed, Standing By

10-11 Talking Too Rapidly
10-12 Visitors Present
10-13 Advise Weather/Road Conditions
10-16 Make Pick Up At _____
10-17 Urgent Business
10-18 Anything For Us?
10-19 Nothing For You, Return To Base
10-20 My Location Is _____
10-21 Call By Telephone
10-22 Report In Person To _____
10-23 Stand By
10-24 Completed Last Assignment
10-25 Can You Contact _____?
10-26 Disregard Last Information
10-27 I Am Moving To Channel _____
10-28 Identify Your Station
10-29 Time Is Up For Contact
10-30 Does Not Conform To FCC Rules
10-32 I Will Give You A Radio Check
10-33 Emergency Traffic At This Station
10-34 Trouble At This Station, Help Needed
10-35 Confidential Information
10-36 Correct Time Is _____
10-37 Wrecker Needed At _____
10-38 Ambulance Needed At _____
10-39 Your Message Delivered
10-41 Please Tune To Channel _____
10-42 Traffic Accident At _____
10-43 Traffic Tieup At _____
10-44 I Have A Message For You (Or _____)
10-45 All Units Within Range Please Report
10-50 Break Channel _____
10-60 What Is Next Message Number?
10-62 Unable To Copy, Use Phone
10-63 Net Directed To _____
10-64 Net Clear
10-65 Awaiting Your Next Message/Assignment
10-67 All Units Comply
10-70 Fire At _____
10-71 Proceed With Transmission In Sequence
10-73 Speed Trap At _____
10-75 You Are Causing Interference
10-77 Negative Contact
10-81 Reserve Hotel Room For _____
10-82 Reserve Room For _____
10-84 My Telephone Number Is _____
10-85 My Address Is _____
10-89 Radio Repairman Needed At _____
10-90 I Have TVI
10-91 Talk Closer To Mike
10-92 Your Transmitter Is Out of Adjustment
10-93 Check My Frequency On This Channel
10-94 Please Give Me A Long Count
10-95 Transmit Dead Carrier For 5 Seconds
10-99 Mission Completed, All Units Secure
10-200 Police Needed At _____

Note. Any 10-Code signal may be reversed by stating it as a question. For example, 10-20? would mean "What is your location?" or 10-36?, "What is the correct time?".

Areas are divided into points or routes. The movement of subject can be followed using these grid or route numbers. When discussing the subject's movements over radio or telephone communications, to insure message security, an approved operations or specially designed code system should be used.

E-5. (U) Example of Transmission

The control point (Bull Durham) and an operating team (Satan) are in communication:

Bull Durham, this is Satan	OVER
Satan, this is Bull Durham	OVER
Bull Durham, this is Satan	SIERRA 53 OVER
Satan, this is Bull Durham	CHARLIE 20 CHARLIE 26 OVER
Bull Durham, this is Satan	ROGER OUT

E-6. (U) Use of Radio Code in Conjunction with a Town Plan or Area Map

Figures E-1 and E-2 illustrate a simple numerical code to show the location and movement of subject.

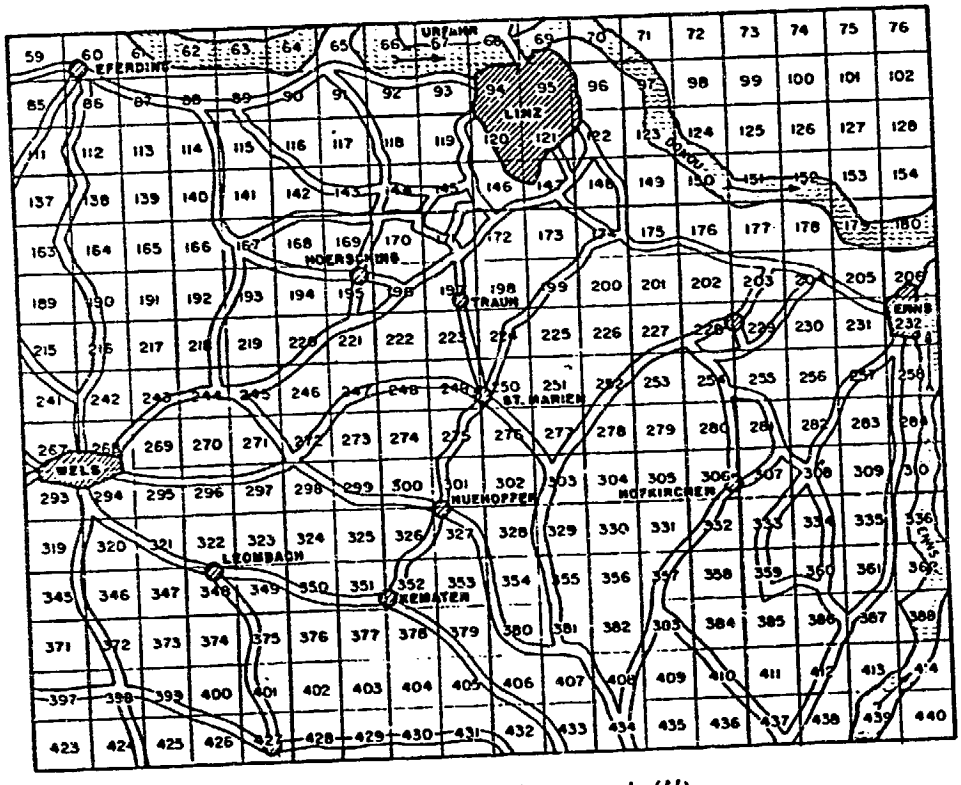


Figure E-1 (U). Grid system code (U).

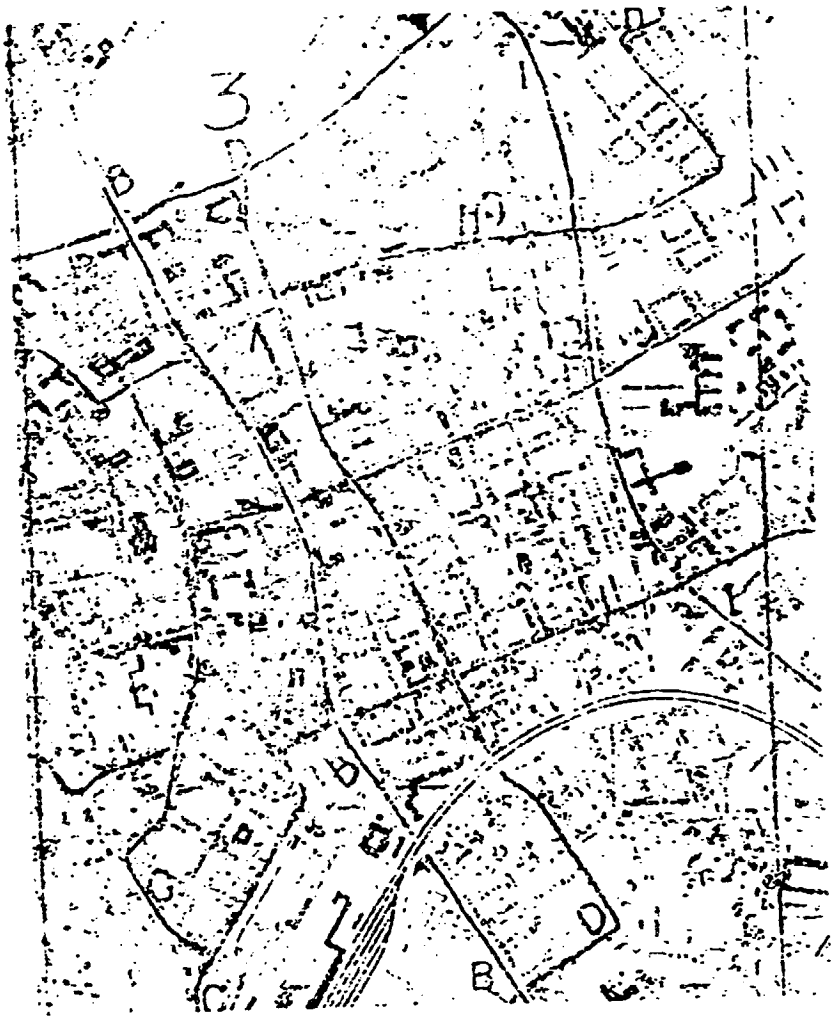


Figure E-2 (U). Point and route system code (U).

E-8. (U) Keyword Code

A simpler point and route system code can be devised using keywords which are easily identifiable and memory associated to aid the surveillants. The following are examples:

a. Palace—Mayor's office or similar high official's or subject's home.

b. Hawaii—Route #50

c. Texas—Supermarket

d. Phillip's—Route #66

e. Phillip's and Hawaii—Intersection of routes 50 and 66.

f. California—West

g. Georgia—South

h. Georgia California—Southwest

By Order of the Secretary of the Army:

CREIGHTON W. ABRAMS
General, United States Army
Chief of Staff

Official:
VERNE L. BOWERS
Major General, United States Army
The Adjutant General

Distribution:
To be distributed in accordance with DA Form 12-11 requirements for Counterintelligence Operations, Intelligence Corps, US Army (U).

U. S. GOVERNMENT PRINTING OFFICE: 1971 O - 498-491

Exempt all pages

FM 30-18 The following pages have been deleted due to classification (Exemption (b)(1)):

1-1 thru 1-2
2-1 thru 2-8
2-11 thru 2-15
3-1 thru 3-8
4-1 thru 4-4
5-1 thru 5-13
6-1 thru 6-9
7-1 thru 7-3
8-1 thru 8-9
9-1 thru 9-5
10-1 thru 10-4
11-1 thru 11-4
12-1 thru 12-8
13-1 thru 13-2
14-1 thru 14-5
15-1 thru 15-4
16-1 thru 16-2
17-1 thru 17-8
18-1 thru 18-2
19-1 thru 19-11
B-1 thru B-29
C-1 thru C-10
D-1 thru D-3
E-1 thru E-3
F-1 thru F-4
G-1
H-1
J-1 thru J-23 (minus J-3)
K-1
Index-1 thru Index-8

~~SECRET~~

FM 30-18

FIELD MANUAL

INTELLIGENCE COLLECTION OPERATIONS (U)

NATIONAL SECURITY INFORMATION
Unauthorized Disclosure Subject to Criminal Sanctions.

HEADQUARTERS, DEPARTMENT OF THE ARMY

NOVEMBER 1973

~~SECRET~~

CLASSIFIED BY: DIAM 58-11(S), 30 June 1965
DEFENSE HUMAN RESOURCES INTELLIGENCE
COLLECTION MANAGEMENT MANUAL (U)
EXEMPT FROM GENERAL DECLASSIFICATION SCHEDULE OF EXECUTIVE ORDER 11652
EXEMPTION CATEGORY: 2
DECLASSIFY ON: CANNOT BE DETERMINED

~~SECRET~~

FM 30-1

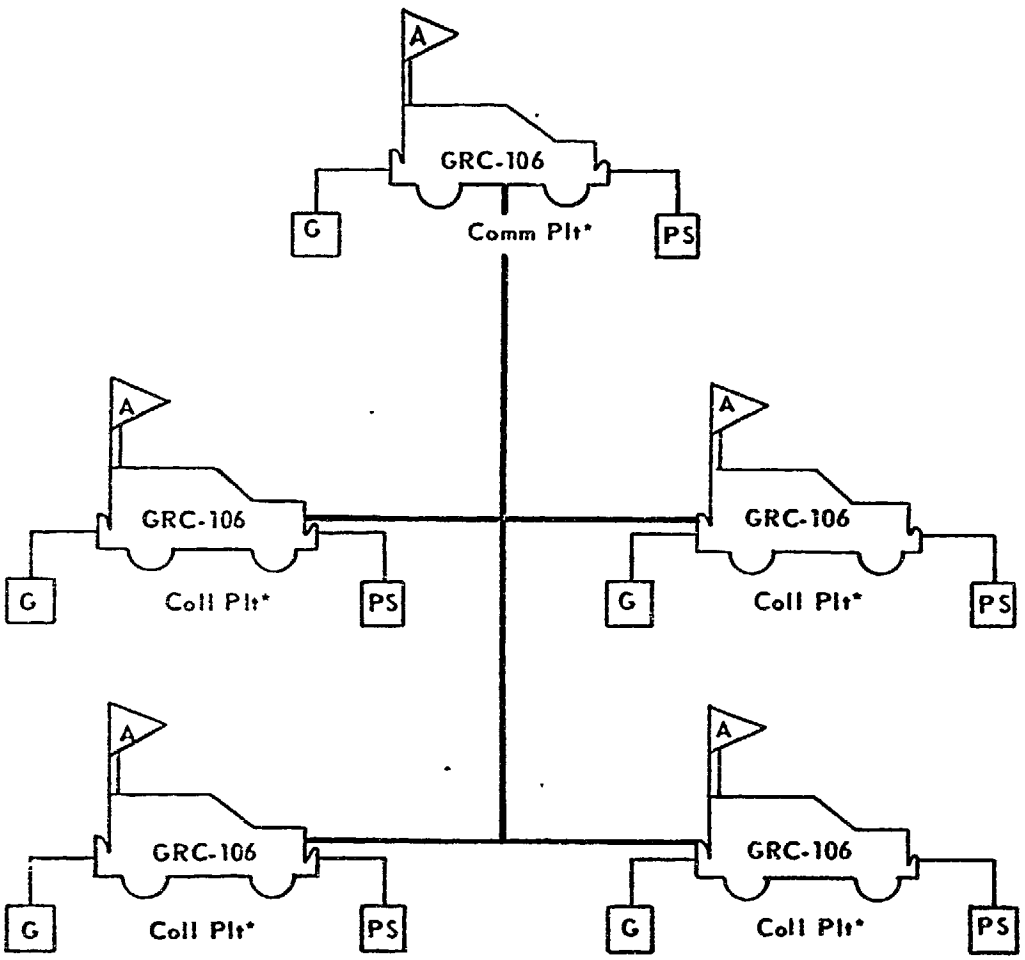
FIELD MANUAL
NO. 30-18

HEADQUARTERS
DEPARTMENT OF THE ARMY
WASHINGTON, D.C., *30 November 1973*

INTELLIGENCE COLLECTION OPERATIONS (U)

This field manual supersedes FM 30-9A, August 1958; FM 30-18, July 1963; and FM 30-31A, August 1967.

~~SECRET~~



* See figure 2-3 for other equipment.

Figure 2-3 (U). Operations monitoring net (CW) (U).

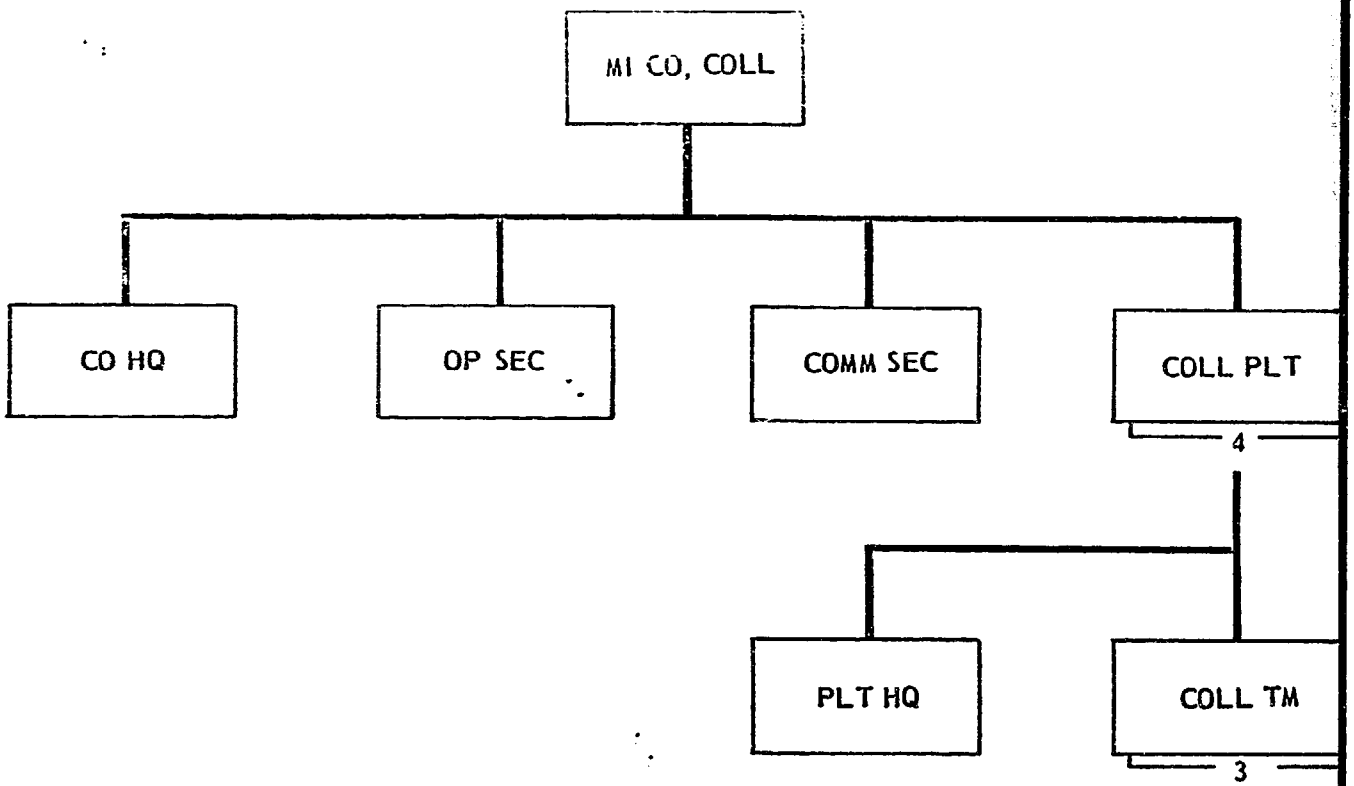


Figure 2-4 (U). MI company collection, theater army (U).

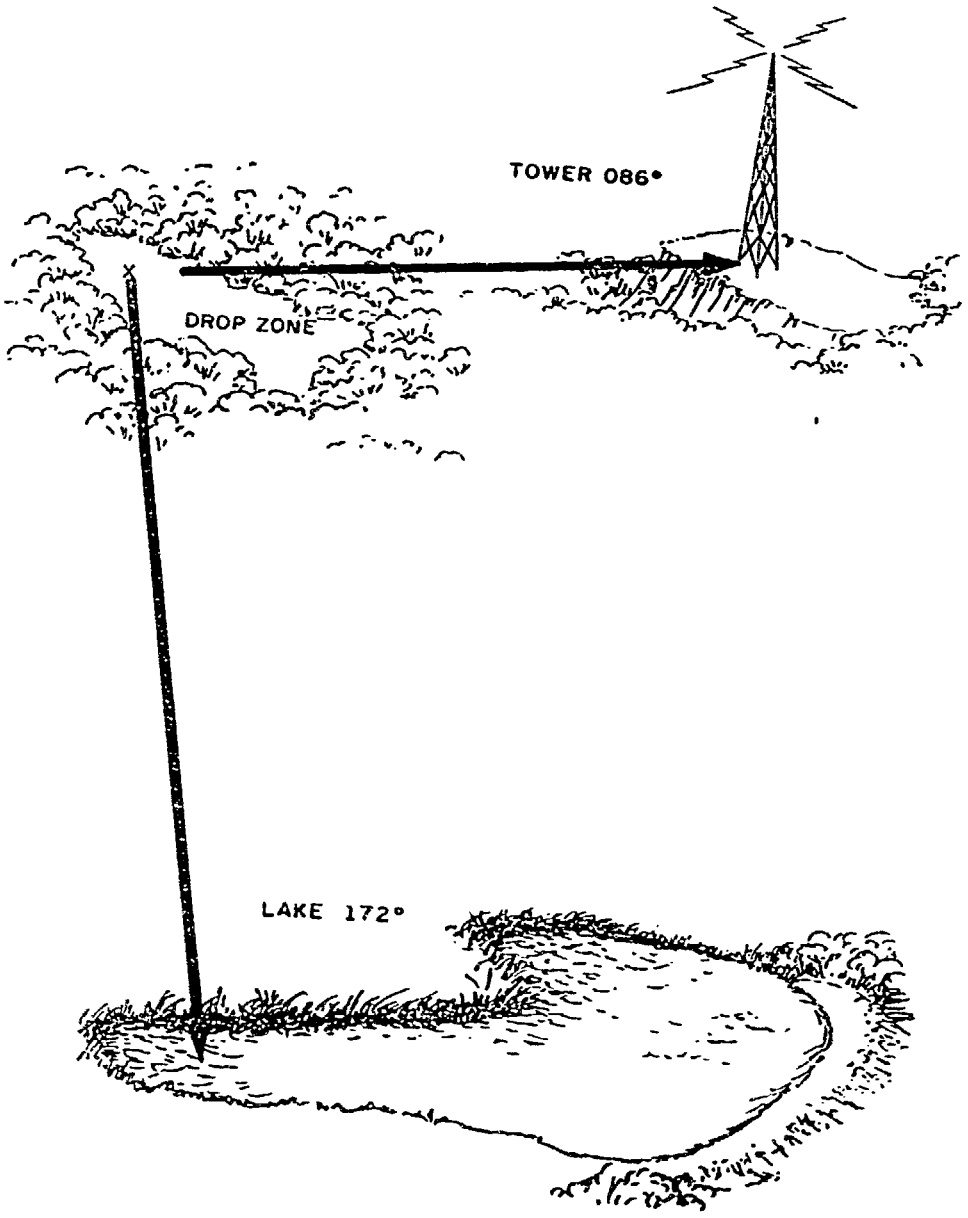


Figure 6–3 (U). Reporting of obstacles and target approach point (U).

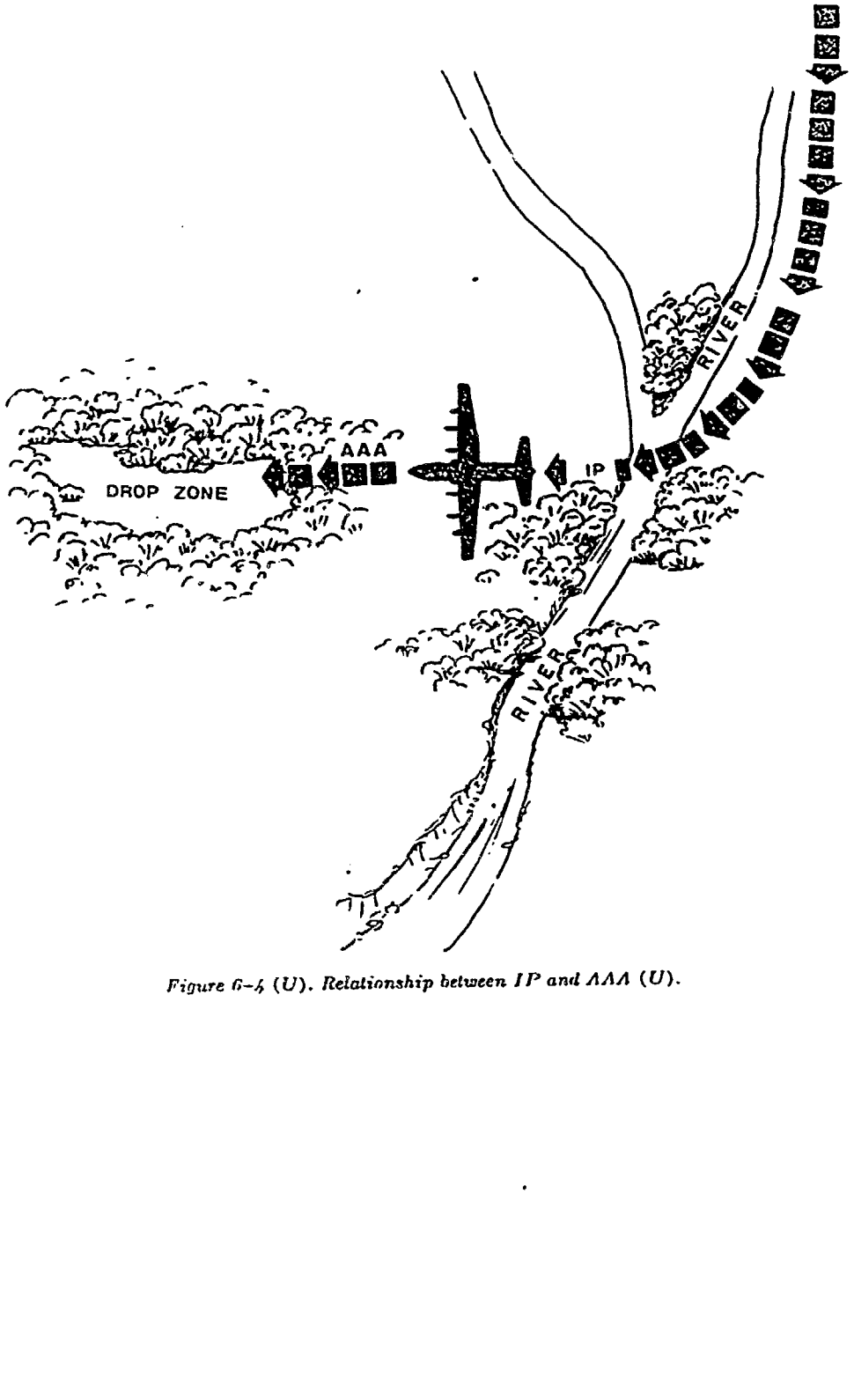


Figure 6-4 (U). Relationship between IP and AAA (U).

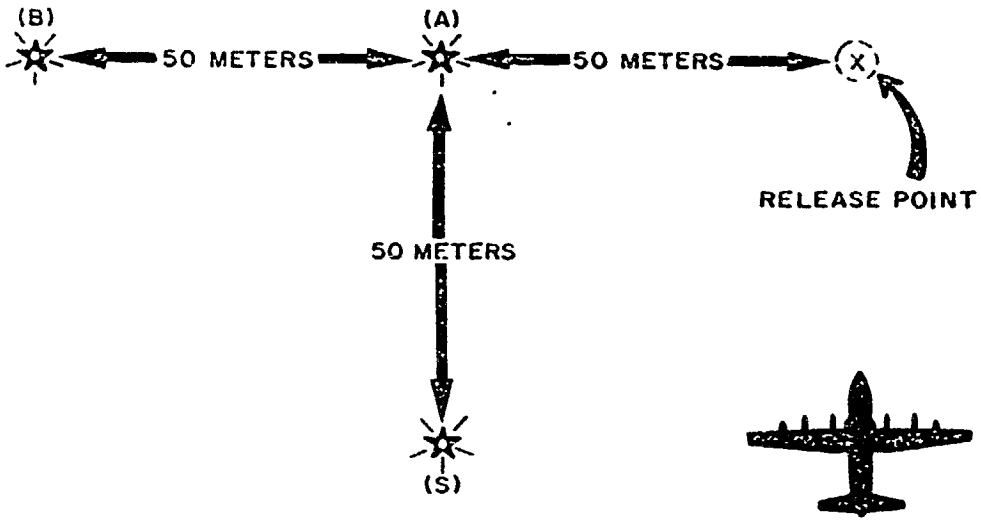


Figure 6-5 (U). Methods of release point marking (U).

APPENDIX A (U)

REFERENCES

AR 105–31	Message Preparation and Processing
AR 135–380	Release of Classified Information to Army National Guard, United States Army Reserve, and Reserve Officers Training Corps
AR 195–6	Department of the Army Polygraph Activities
AR 310–25	Dictionary of United States Army Terms
AR 310–50	Authorized Abbreviations and Brevity Codes
AR 340–2	Maintenance and Disposition of Records in TOE Units of the Active Army and Army Reserve
AR 340–15	Preparing Correspondence
AR 340–16	Safeguarding Nondefense Information
AR 380–series	Security
AR 381–series	Military Intelligence
AR 405–10	Acquisition of Real Property and Interests Therein
AR 600–3	Women's Army Corps—General Provisions
(FOUO) AR 614–31	Assignment and Travel Restrictions
(C) AR 614–32	Restrictions of Assignment and Travel of Personnel Having Access to Special Intelligence (U)
AR 640–20	US Army Intelligence Badges and Credentials
AR 715–30	Local Purchase of Civilian Type Items
AR 930–5	American National Red Cross Service Program and Army Utilization
DA Pam 27–1	Treaties Governing Land Warfare
FM 30-series	Military Intelligence
(S) FM 31–21A	Special Forces Operations (U)
FM 31–73	Advisor Handbook for Stability Operations
FM 32–5	Signal Security (SIGSEC)
(S) FM 32–10	USASA in Support of Tactical Operations (U)
(C) FM 32–20	Electronic Warfare (U)
(S) FM 101–10–3	Staff Officers' Field Manual, Organizational, Technical, and Logistical Data, Classified Data (U)
TM 11–401	Elements of Signal Photography
TM 30-series	Military Intelligence
TOE 30-series	Military Intelligence
DIAM 58–11	Human Resources Intelligence Collection Management Manual, Volumes I and II (DIHUM and DICOM)

APPENDIX I (S)

MINIMUM REQUIREMENTS FOR SENSITIVE PROJECT CONCEPT OR PROPOSAL

(May be modified as necessary)

1. (U) Identification Data

a. Originating headquarters.
b. Date originated.
c. Project code name.
d. Target country or countries.
e. Reference IIRCD and/or CCOL objectives/ equirements to which proposed project pertains.

Section II. INTELLIGENCE INFORMATION REPORTS GENERAL INSTRUCTIONS—BODY OF REPORT

J-5. (U) Report Organization

The body of the report will be started at the left margin immediately below the dashed line on DD Form 1396. All of the space between the vertical margin lines on DD Forms 1396 and 1396c will be used. Paragraphs must be numbered if there are more than one. Paragraphing and subparagraphing must conform to usual military correspondence practice. The abbreviated classification for each paragraph must be inserted in parentheses after the number of each paragraph. When using standardized format (military and industrial installation reports) the paragraph number, abbreviated classification symbol in parentheses and the paragraph heading in underlined upper case letters must be included. The narrative is continued on DD Forms 1396c, using as many as necessary to complete the report. Overlays and sketches, together with their legends, immediately follow the text, also using DD Forms 1396c. Attachments are placed after sketches.

By Order of the Secretary of the Army:

CREIGHTON W. ABRAMS
General, United States Army
Chief of Staff

Official:
VERNE L. BOWERS
Major General, United States Army
The Adjutant General

Distribution:
To be distributed in accordance with DA Form 12–11B requirements for Intelligence Collections Operations, Intelligence Corps, USA (U) (Qty Rqr Block No. 282).